Configuring Interface and Router Redundancy

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114079 Rev. A
August 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Configuring Interface and Router Redundancy

About This Guide

Before You Begin xiii
Conventions xiv
Acronyms xv
Ordering Bay Networks Publications xv

Technical Support and Online Services

Bay Networks Customer Service xviii
Bay Networks Information Services xix
World Wide Web xix
Customer Service FTP xix
Support Source CD xx
CompuServe xx
InfoFACTS xxi
How to Get Help xxi

Chapter 1
Interface Redundancy Overview

Active Interface 1-1
Redundant Interfaces 1-1
Interface Roles 1-2
Determining the Active Interface 1-2
Reset Active Feature 1-2
Determining Priority 1-2
Role Change Speed on Ethernet 1-3
Hot and Warm Standby 1-3
Hot Standby 1-3
Warm Standby 1-3

Active Interface MAC Address 1-4

Chapter 2
Router Redundancy Overview

Primary Router 2-1
Dedicated Secondary Router 2-1
Redundancy Protocol 2-2
Role Change 2-6
Router Failure 2-6
Interface Failure 2-6
Speed of Failed Interface Detection for Ethernet 2-6
Resource Availability 2-6
Bypassing the Bidding Process 2-7

Chapter 3
Implementation Notes

Planning Your Network 3-1
Protocols Supported 3-2
LAN Interfaces 3-2
Router Redundancy Requirements 3-2
Using Interface and Router Redundancy in Combination 3-3
Clear Function 3-4
Compatibility 3-4

Chapter 4
Configuring Interface Redundancy

Enabling Interface Redundancy 4-1
Adding and Deleting Interfaces within a Group 4-5
Removing Interface Redundancy from a Circuit 4-6

Chapter 5
Configuring Router Redundancy

Enabling Router Redundancy 5-2
Creating a Group Configuration File 5-2
Router Redundancy Group Global Parameter Descriptions 5-7
Configuring Resources 5-11
Router Redundancy Resource Parameter Descriptions 5-13
Applying a Group Configuration File 5-15

Router Redundancy Member Global Parameter Descriptions 5-18
Sending the Configuration Files to the Routers 5-21
Removing Router Redundancy 5-21

Appendix A
Site Manager Default Parameter Settings

Appendix B
Router Redundancy Examples

Example 1: Two Routers at the Same Site B-1
Router Bootup B-1
Possible Scenarios B-2
Secondary Router Degraded B-2
Secondary Router Becomes Inoperable B-2
Primary Router Degraded B-2
Primary Router Fails B-2
Possible Complications B-3
Router Boots and Cannot Detect Another Member B-3
Second Router Boots After First Router's Bidding Timer Expires B-3
Manual vs. Auto Role Switching B-3
Example 2: Three Routers at the Same Site B-4
Example 3: Router Redundancy with Wide Area Networks B-5

Appendix C
Worksheets for Configuring Router Redundancy

Index

Figures

Figure 4-1. Add Circuit Window 4-2
Figure 4-2. Edit Connector Window 4-3
Figure 4-3. Circuit Definition Window 4-3
Figure 4-4. Select Primary Window 4-4
Figure 4-5. Circuit Definition Window with Primary Interface 4-5
Figure 5-1. Main Site Manager Window 5-3
Figure 5-2. Add Circuit Window 5-4
Figure 5-3. Select Protocols Window 5-5
Figure 5-4. Router Redundancy Circuit Window 5-5
Figure 5-5. R.R. Group Global Parameters Configuration Window 5-6
Figure 5-6. RREDUND Router Redundancy Resource List Window 5-12
Figure 5-7. Router Redundancy Resource Window 5-12
Figure 5-8. Configuration Manager Window in Member Mode 5-15
Figure 5-9. Configuration Manager Window for Member Configuration 5-16
Figure 5-10. R.R. Member Global Parameters Configuration Window 5-17
Figure 5-11. Save Configuration File Window 5-17
Figure B-1. Router Redundancy: Two Routers at the Same Site B-1
Figure B-2. Router Redundancy: Three Routers at the Same Site B-4
Figure B-3. Router Redundancy with Wide Area Networks B-5

Tables

Table 2-1. Redundancy Protocol PDU Flow Diagram for Role Bidding 2-2
Table 2-2. Redundancy Protocol PDU Flow Diagram for SOS PDUs 2-5
Table 3-1. Using Interface Redundancy across Slots with Router Redundancy 3-3
Table A-1. Router Redundancy Group Global Parameters A-1
Table A-2. Router Redundancy Member Global Parameters A-2
Table A-3. Router Redundancy Resource Parameters A-2
Table C-1. Group Mode Planning Worksheet C-1
Table C-2. Resource Planning Worksheet C-2
Table C-3. Member Mode Planning Worksheet C-2

About This Guide

Bay Networks™ redundancy services enhance router resilience by enabling a router to recover from either interface or router failure with minimal delay.

Interface redundancy protects your network from failures of individual LAN interfaces on a router. Router redundancy protects your network from failures of the entire router. You can use these services separately or in combination to ensure smooth and continuous operation of your network.

Configuring Interface and Router Redundancy offers

- Overviews of interface and router redundancy and descriptions of how Bay Networks redundancy services work (Chapter 1 and Chapter 2)
- Implementation notes that may affect how you configure interface and router redundancy (Chapter 3)
- Instructions on configuring interface redundancy (Chapter 4)
- Instructions on configuring router redundancy (Chapter 5)
- Tables of default parameter values for router redundancy (Appendix A)
- Examples of how you can use router redundancy in your network (Appendix B)
- Worksheets to help you configure router redundancy (Appendix C)

Before You Begin

Before using this guide, you must complete the following procedures:

- Create and save a configuration file.
- Retrieve the configuration file in local or remote mode.

Refer to *Configuring Routers* for instructions.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–10.xx to Version 11.0*.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

BOFL	Breath of Life
FDDI	Fiber Distributed Data Interface
IP	Internet Protocol
IPX	Internet Packet Exchange
LAN	local area network
MAC	Media Access Control
MIB	Management Information Base
OUI	organizationally unique identifier
PDU	protocol data unit
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Interface Redundancy Overview

Interface redundancy provides backup of one interface by another within a single router. It protects your network from partial router or installation failures; it also enables you to maintain data transmission for critical interfaces without the expense of two routers.

You configure interfaces to be members of an *interface redundancy group*. The group includes an *active interface,* which performs normal routing and bridging services, and one or more *redundant interfaces*, which take over if the active interface fails.

You can configure multiple interface redundancy groups on the same router.

Active Interface

The active interface performs normal bridging and routing services.

When you configure interface redundancy, you can select one interface on the router to have the highest priority to be the active interface. That interface is the *designated primary interface*. Under normal circumstances, the designated primary interface is the active interface for the redundancy group. If the active interface fails, however, another interface in the group becomes the new active interface.

Redundant Interfaces

All members of an interface redundancy group other than the active interface are redundant interfaces. A redundant interface has no function other than to serve as a backup.

Interface Roles

Bay Networks interface redundancy software determines which interface in a redundancy group becomes the active interface if the current active interface fails. The software also determines the priority for each of the remaining members of the group to become the active interface.

Determining the Active Interface

When you boot a router configured with interface redundancy, the designated primary interface has 12 seconds to become active. If it does become active, data transmission begins normally.

If the designated primary interface does not become active within 12 seconds, the redundant interface with the highest priority becomes the active interface, and transmission begins. The 12-second initialization period occurs only once, and applies only to the designated primary interface. After initialization, all redundant interfaces are ready to become active immediately if the active interface fails.

Reset Active Feature

Interface redundancy includes a Reset Active feature that allows you to force the interface you have designated as primary to become the active interface. Using this feature may improve network performance. Refer to Chapter 4 for information about accessing the Reset Active feature.

Determining Priority

The redundant interface with the highest priority becomes the active interface if the active interface fails.

During startup, if the designated primary interface fails to become active, the following interfaces become active, in this order:

1. Redundant interfaces on the same slot as the designated primary interface
2. Redundant interfaces on other slots

During normal data transfer, if the active interface fails, the following interfaces become active, in this order:

1. Redundant interfaces on the slot that is processing the routing/bridging table for this circuit
2. Redundant interfaces on other slots

Role Change Speed on Ethernet

To increase the speed of detecting failed interfaces and changing roles on Ethernet connectors, set the BOFL Timeout parameter to a short interval, such as one second. The cost is LAN bandwidth and CPU overhead. To access the BOFL Timeout parameter, select Line > Edit Lines in the Circuit Definition window. For further information, refer to *Configuring Line Services*.

Hot and Warm Standby

When a redundant interface takes over for a failed interface without interruption in service, it does so under one of two conditions: *hot standby* or *warm standby.*

Hot Standby

When the active interface fails, but the circuit is still up, the new active interface retains access to the routing/bridging tables, and can continue transmission immediately.

Only if the routing/bridging tables are on another slot from the new active interface is there any loss in performance. The priority rules for interfaces to become active operate to avoid this situation whenever possible.

Warm Standby

When the active interface fails and the circuit has gone down, the CPU module processing the routing/bridging table is at fault, and the router loses the routing/bridging tables.

Transmission continues, but is slower than in the case of hot standby, because the new active interface must relearn the routing/bridging tables.

Active Interface MAC Address

When you configure interface redundancy, the active interface uses the following MAC address in hexadecimal radix:

0x2000 A2*xx xxxx*

- 0x20 indicates that the address is locally administered by Bay Networks.
- 00A2 identifies the Bay Networks organizationally unique identifier (OUI).
- *xx xxxx* is the unique router identification number.

The active interface in an interface redundancy group uses the MAC address for all traffic, including Breath of Life (BOFL). The MAC address switches among interfaces in the interface redundancy group so that it always represents the active interface.

The MAC address affects network layer protocol adjacent host setups on adjacent routers. For example, if you have adjacent routers and the IP adjacent host is defined with its next hop being the active interface in an interface redundancy group, the adjacent host MAC address must be the active interface's MAC address, that is, **0x2000 A2*xx xxxx***.

You can find the complete MAC address for the active interface in the interface MIB (Ethernet, Token Ring, FDDI) of the router on which interface redundancy is configured. For example, if you are configuring Ethernet, you can find the active MAC address in the Ethernet MIB by entering the following command from the Technician Interface:

get wfCSMACDEntry.wfCSMACDMadr.*

Among the entries displayed in the MIB is the MAC address **0x2000 A2*xx xxxx,*** which is used for interface redundancy. If you configure more than one interface redundancy group on the same router, you will see more than one entry with the same MAC address. This is not a problem because the two redundancy groups are in different subnets.

Chapter 2
Router Redundancy Overview

Router redundancy protects a network from irrecoverable failures of an entire router. You configure routers to be members of a *router redundancy group*. The group includes a primary router that performs normal routing and bridging services, and one or more secondary routers that take over if the primary router fails.

Note: You can configure multiple router redundancy groups on the same network.

Primary Router

Bay Networks router redundancy software allows you to decide which router has priority to be the primary router, and includes configurable bidding timers and timeout periods that determine how and when a router in a redundancy group changes roles from secondary to primary.

Dedicated Secondary Router

Bay Networks recommends that you configure router redundancy so that a secondary router has no function other than to serve as a backup. A router so configured is a *dedicated secondary router*.

You can configure a redundant router to carry other traffic, unrelated to that of its redundancy group. Be aware, however, that if a secondary router becomes the primary router in a redundancy group, it reboots and stops any other data transfer it was performing. When you configure a router as a member of a router redundancy group, its role in that group takes precedence over any other functions you assign it.

Redundancy Protocol

Routers in a redundancy group all begin in the secondary role.

A router assumes the primary role according to the following criteria, and the redundancy protocol considers the criteria in the following order. For example, if two routers in a router redundancy group have the same number of good interfaces, the protocol considers the number of reachable resources each router has. But if one router has a larger number of good interfaces, that router becomes primary without consideration of subsequent criteria.

1. Number of good interfaces
2. Number of reachable resources
3. Priority to become primary, which you configure
4. Lowest member ID (for further information, see the Member ID parameter in Chapter 5)

The routers use a bidding process to determine which router becomes the primary router. If the group has more than two members, the bidding process also determines which of the backup routers is the best secondary router. The bidding process consists of an exchange of messages called *protocol data units* (PDUs).

Table 2-1 provides a detailed description of this process.

Table 2-1. Redundancy Protocol PDU Flow Diagram for Role Bidding

Router A	PDU	Router B
Starts in secondary role.		Starts in secondary role.
Sends Hello PDUs at periodic intervals. These PDUs start the bidding for the primary role.	Hello PDU Role = Secondary ---------->	Receives Hello PDU from Router A and stores its contents in the redundancy group database. Checks to see if Router A is a better primary router; if so, Router B does not plan to change roles.
Receives Hello PDU from Router B and stores its contents in the redundancy group database. Checks to see if Router B is a better primary router; if so, Router A does not plan to change roles.	Hello PDU Role = Secondary <----------	Starts sending Hello PDUs at periodic intervals; these PDUs are Router B's bids for the primary role.

Table 2-1. Redundancy Protocol PDU Flow Diagram for Role Bidding *(continued)*

Router A	PDU	Router B
After the bidding period times out, it is determined that Router A is the best primary router. Router A sends out the SOS New Primary PDU, then performs the role-changing action to become the primary router.	SOS New Primary PDU Role = Secondary ---------->	After the bidding period times out, it is determined that another member of the router redundancy group is the best primary router. Router B remains in a secondary role and continues to monitor the redundancy group status.
Receives the periodic Hello PDU and updates the redundancy group database, including each member's interface status information.	Hello PDU Role = Secondary <----------	Continues sending periodic Hello PDUs with local interface status information.
Continues sending periodic Primary Hello PDUs with local interface status information. The Primary Hello PDUs from the primary router have additional meaning to other members of the redundancy group.	Hello PDU Role = Primary ---------->	Receives the periodic Primary Hello PDUs and updates the redundancy group database, including each member's interface status information. Restarts the Primary OK Timer.
	Time Passes	
Primary router fails. Router A is in an unknown state; may not have received this PDU.	SOS New Primary PDU Role = Secondary <----------	Primary OK Timer expires for *n* times. Router B determines that the primary router has failed. Based on information in the redundancy group database, it is determined that Router B is the best secondary router to become the new primary router. Router B sends an SOS New Primary PDU, which prevents any other secondary router in the group from becoming the primary router. Router B becomes the new primary router.
Router A remains in an unknown state; may not have received this PDU.	Hello PDU Role = Primary <----------	As the new primary router, Router B periodically sends Primary Hello PDUs with local interface status information.

The primary router periodically checks that it is functioning normally. If the primary router is not functioning properly, a role change occurs, as follows:

1. The primary router notifies the best secondary router that it intends to change out of the primary role.
2. The best secondary router informs the other members of the impending role change, and those members start a timer (using the Bidding Timer value) to prevent additional role changes by other members.
3. The best secondary router reboots, using the primary configuration file, and assumes primary status.

Table 2-2 describes how a primary router changes to a secondary role while the best secondary router assumes the primary role.

Table 2-2. Redundancy Protocol PDU Flow Diagram for SOS PDUs

Router A	PDU	Router B
Router A, currently the primary router, sends Primary Hello PDUs at periodic intervals.	Hello PDU Role = Primary ---------->	Router B, currently a secondary router, receives the periodic Primary Hello PDUs and updates the redundancy group database. Router B restarts the Primary OK Timer.
Receives the periodic Hello PDUs and updates the redundancy group database.	Hello PDU Role = Secondary <----------	Router B sends out periodic Hello PDUs.
Router A detects local partial failures; for example, an important interface has failed. Router A knows that Router B is a better primary router, so Router A plans to change its role to secondary. Router A issues an SOS PDU to inform all members of the redundancy group of its intention to change out of the primary role.	SOS PDU Role = Primary ---------->	Router B, the best secondary router, receives the SOS PDU. Router B confirms that it is the best secondary router by sending the SOS Reply PDU.
Router A, the current primary router, receives the SOS Reply PDU with its OK indication from Router B.	SOS Reply PDU Role = Secondary <----------	Router B sends the SOS Reply PDU, indicating that it is ready to be the new primary router, and that it is OK for the current primary router to change out of the primary role.
Router A sends an SOS Primary Goodbye PDU, then changes out of the primary role.	SOS Primary Goodbye PDU Role = Primary ---------->	Router B receives the SOS Primary Goodbye PDU.
Router A may not receive this PDU, but all other members of the redundancy group do. This message tells the other secondary members to delay bidding for the new primary role until after the bidding timer expires and they detect that there is no primary router.	SOS New Primary PDU Role = Secondary <----------	Router B sends the SOS New Primary PDU to indicate that it is changing roles to become the new primary router. Router B changes its role to become the new primary router.
Router A may not receive this PDU. All other members of the redundancy group do, and update their redundancy group databases.	Hello PDU Role = Primary <----------	Router B has finished with the role change and is now the new primary router. Router B sends its first periodic Primary Hello PDU.

Role Change

A router may change out of the primary role because of router failure, failure of one or more interfaces, or because it cannot reach its resources.

Router Failure

If the primary router in a router redundancy group fails entirely, it obviously is no longer the best primary router, and a role change occurs, as outlined in Table 2-1 and Table 2-2.

Interface Failure

If one or more interfaces on the primary router fail, it is probably no longer the best primary router, depending on the status of the interfaces on the other routers in the router redundancy group. If it is not the best primary router, it changes out of the primary role.

Speed of Failed Interface Detection for Ethernet

To increase the speed of detecting failed interfaces and changing roles on Ethernet connectors, set the BOFL Timeout parameter to a short interval, such as one second. The cost is LAN bandwidth and CPU overhead. To access the BOFL Timeout parameter, select Lines > Edit Lines in the Circuit Definition window. For further information, refer to *Configuring Line Services*.

Resource Availability

A router is functioning normally if it can reach the resources -- servers, printers, and other devices -- with which you configure it to communicate. If a primary router in a redundancy group cannot reach its resources, it changes out of the primary role. Resources are determined by IP address, so all resources must be running TCP/IP.

Bay Networks redundancy software includes several parameters that allow you to control how often and how many times a router attempts to ping its resources (see Chapter 5).

Bypassing the Bidding Process

If your secondary router is performing network functions and you want the primary router to assume these functions after it switches out of the primary role, the primary and secondary configuration files for both routers must be identical. The only parameters that are different between the two routers are the primary configuration file name and the member ID.

You must also boot the primary router directly into its primary configuration, and the secondary router into its secondary configuration, bypassing the bidding process. Failure to do so can result in connection problems related to both routers having the same IP address on a LAN.

Chapter 3
Implementation Notes

This chapter provides information about special features of Bay Networks interface and router redundancy.

Planning Your Network

Configuring router redundancy on your network is somewhat different from configuring most protocols, because router redundancy involves multiple nodes. Consider your network requirements and design your interface and router redundancy groups carefully to maximize the benefits of using redundancy. In particular, keep in mind the following characteristics of router and interface redundancy:

- The interfaces you configure as backed-up interfaces should perform routing services that you rate as your highest priority.
- Remember that if a router becomes the primary router in a router redundancy group, other functions it has been performing while in the secondary role terminate.
- Bay Networks recommends that you configure redundant routers as dedicated redundant routers, that is, with the backup role as their sole function.
- A router can be a member of only one router redundancy group.

When planning your network for router redundancy, follow these guidelines:

1. Determine the backed-up interfaces in each member of the router redundancy group.
2. Select the group ID and member IDs for router redundancy, noting the following:
    a. The group ID must be unique for each group in the network.

b. Each member ID must be unique within the group. Role-changing rules use the member IDs to reassign roles. When two routers have the same priority, the one with the lowest member ID becomes the primary router when a role change occurs.

3. Use more than one interface as the backup interface for router redundancy. This procedure avoids a single point of failure.

Refer to Appendix C for worksheets to help you plan your router redundancy group.

Protocols Supported

Interface and router redundancy work with IP, IPX, Spanning Tree Bridging, and Source Route Bridging. Interface redundancy also works with AppleTalk and VINES.

LAN Interfaces

Interface and router redundancy support the following LAN interfaces as redundant interfaces: 10-Mb Ethernet, 100-Mb Ethernet, Token Ring, and FDDI.

All members of an interface redundancy group must be LAN interfaces of the same type.

Multiple LAN interfaces of the same type or different types can carry the router redundancy protocol.

Router Redundancy Requirements

All members of a router redundancy group must

- Be the same router type; for example, BCN®, BLN®, or ASN™.
- Have the same hardware configuration. This includes CPU and interface module types, and slot and port locations of the backed-up interfaces.
- Have the same software configuration. For example, you must be running the same router software version and have the same loadable modules configured.

Using Interface and Router Redundancy in Combination

Use interface redundancy with router redundancy to provide combined protection from internal router failure and total router failure. The combination of interface and router redundancy provides better interface protection than is possible using interface redundancy alone.

You can configure backed-up interfaces within redundant routers, and you can also configure some interfaces that are not backed up. Interface redundancy allows data transmission to occur without interruption in the event of a failed interface. Router redundancy provides the security of uninterrupted network service.

Caution: If you configure interface redundancy across slots with router redundancy, and the CPU board for the slot with the active interface fails, router redundancy may take precedence over interface redundancy, even though there is a member of the interface redundancy group available to transmit data. The result will be unnecessary delays in data transmission.

Table 3-1 demonstrates what happens when you configure interface redundancy across slots when you are using router and interface redundancy together.

Table 3-1. Using Interface Redundancy across Slots with Router Redundancy

Router A	Router B
Router A is in the primary role for router redundancy. It also has the active interface in the interface redundancy group.	Router B is in the secondary role.
The CPU board for the active interface fails. Router A detects that it is no longer the best primary router, so Router A changes its role to secondary.	Router B is the new best primary router, and it assumes the primary role. To do so, it reboots, using the primary configuration file.
Meanwhile, a redundant interface from the interface redundancy group has become active, with the result that Router A is again the best primary router in the router redundancy group.	Router B recognizes that it is no longer the best primary router and switches out of the primary role.
Router A assumes the primary role. To do so, it reboots, using the primary configuration file.	Router B is in the secondary role.
Data is again moving, but with delays for rebooting.	

Clear Function

The Clear function allows you to clear all protocols from all circuits that have router redundancy configured. The Clear function does not clear any protocols from circuits that are not configured for router redundancy. This feature is useful when you convert a primary router redundancy configuration to a secondary configuration, because a typical secondary configuration does not include any of the protocols that the primary has.

Access the Clear function from the Protocols > Router Redundancy menu in the Configuration Manager main window.

Compatibility

Interface redundancy was introduced with Bay Networks Software Version 9.00/3.00, and router redundancy was a new feature of Bay Networks Software Version 10.0/4.0. Neither is compatible with earlier versions of our router hardware and software, or with the products of other vendors.

Chapter 4
Configuring Interface Redundancy

This chapter describes how to configure interface redundancy. It assumes you have read *Configuring Routers* and Chapter 1 and Chapter 3 of this guide, and that you have

1. Opened a configuration file in local or remote mode
2. Specified router hardware if this is a local mode configuration file
3. Selected the link- or net-module connector on which you are enabling interface redundancy

To enable interface redundancy, you must select at least two interfaces as members of an interface redundancy group. One of the interfaces is the designated primary interface; under normal circumstances it is the active interface that provides normal routing/bridging services. The other is the redundant interface; it takes over if the active interface fails.

Enabling Interface Redundancy

To configure an interface redundancy group:

1. **In the Configuration Manager window, select an available LAN interface.**

   The Add Circuit window appears (Figure 4-1).

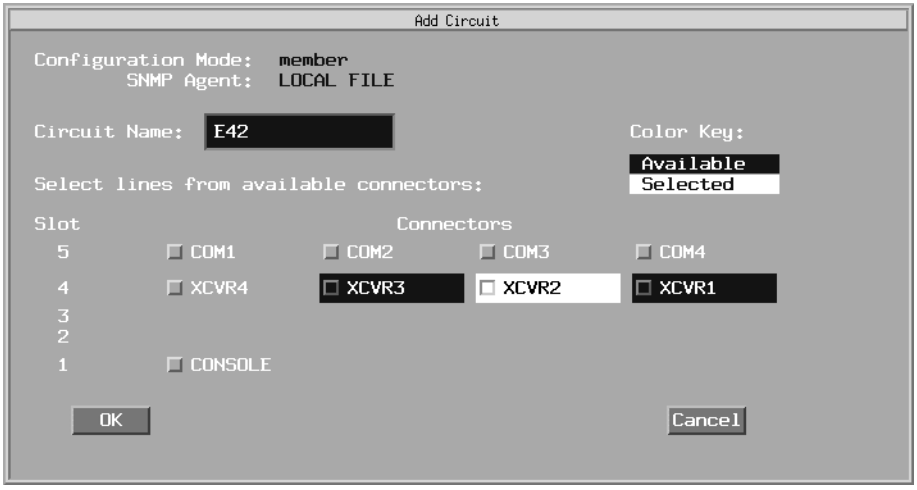

Figure 4-1. Add Circuit Window

2. **Select all other available LAN interfaces of the same type that you want to be members of this interface redundancy group.**
3. **Click on OK.**

   Interface redundancy is now enabled on this circuit. The Select Protocols window appears.
4. **Select the protocols you want to configure on the circuit. When you are done, click on OK.**
5. **Repeat Steps 1 through 4 to create additional interface redundancy groups.**
6. **In the Configuration Manager window, select one of the connectors in the interface redundancy group you just created.**

   The Edit Connector window appears (Figure 4-2).

Figure 4-2. Edit Connector Window

7. **Select Edit Circuit. The Circuit Definition window appears (Figure 4-3).**

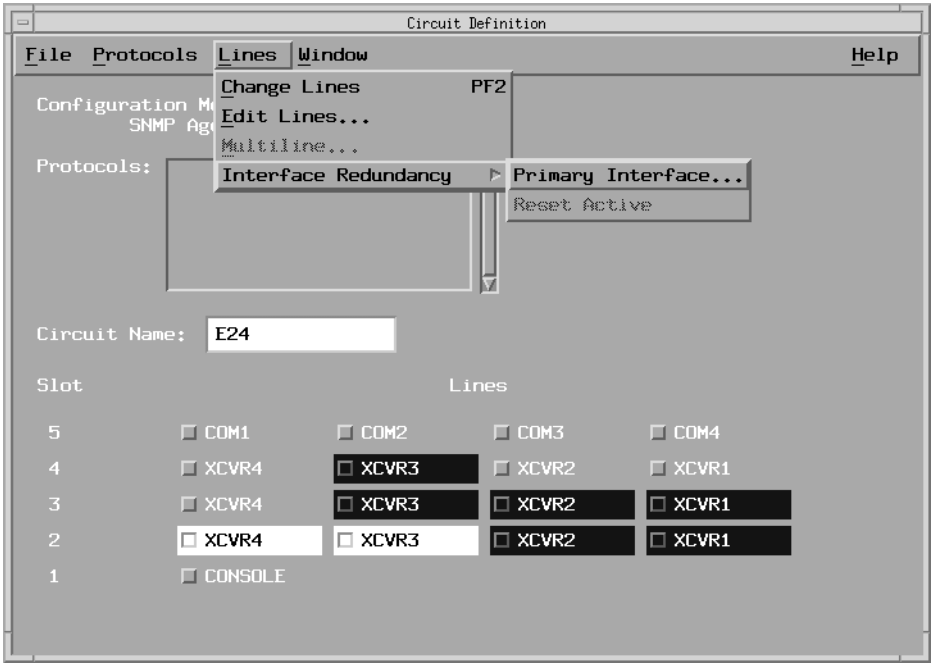

Figure 4-3. Circuit Definition Window

Note: The Reset Active option below Lines > Interface Redundancy > Primary Interface is available in dynamic mode only. This option allows you to force the interface you have designated as primary to become the active interface. Using this option may improve performance.

8. **In the Circuit Definition window, select Lines > Interface Redundancy > Primary Interface.**

   The Select Primary window appears (Figure 4-4).

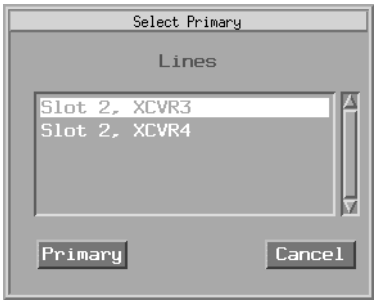

Figure 4-4. Select Primary Window

9. **Select an interface from the list in the Select Primary window, and click on Primary.**

   Site Manager redisplays the Circuit Definition window with the letter P now appended to the interface you designated as primary (Figure 4-5).

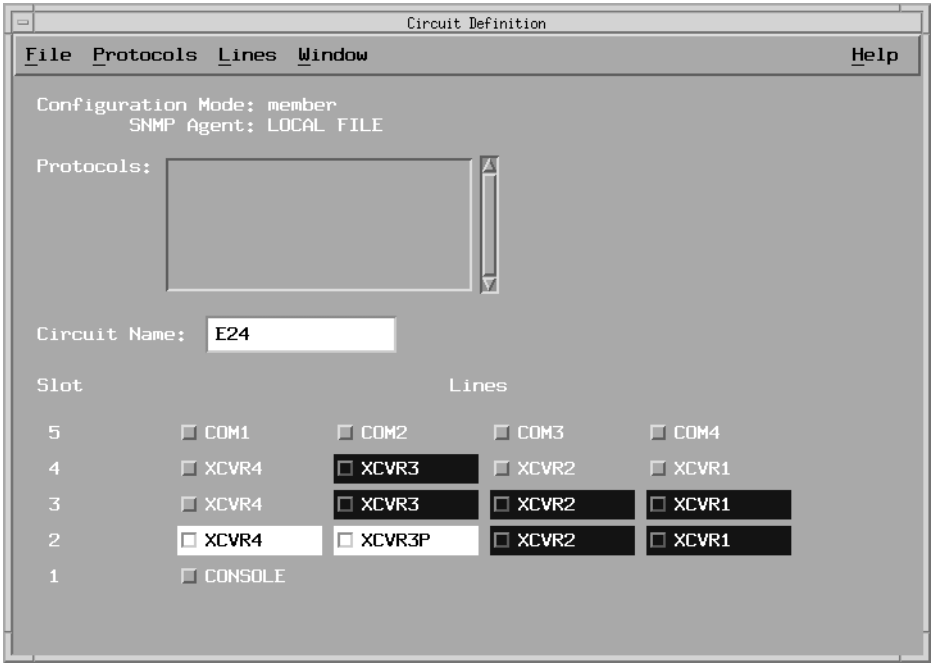

Figure 4-5. Circuit Definition Window with Primary Interface

10. **Select File > Exit to exit the Circuit Definition window and return to the Configuration Manager window.**

Adding and Deleting Interfaces within a Group

To add an interface to an existing interface redundancy group or to delete an interface from a group:

1. **In the Configuration Manager window, select any circuit in the group that you want to change.**

   The Edit Connector window appears (refer to Figure 4-2).

2. **Click on Edit Circuit.**

   The Circuit Definition window appears (refer to Figure 4-3).

3. **To add an interface, select an available line of the same LAN type as the other members of the group. To delete an interface, select the line you wish to delete from the group.**
4. **Select Lines > Change Lines.**

   The interface you selected is now added to or deleted from the interface redundancy group. If only one interface remains on the circuit, the interface redundancy group no longer exists.

Removing Interface Redundancy from a Circuit

To remove interface redundancy from a circuit:

1. **In the Configuration Manager window, select any member of the interface redundancy group you want to remove.**

   The Edit Connector window appears (refer to Figure 4-2).
2. **Select Edit Circuit.**

   The Circuit Definition window appears (refer to Figure 4-3).
3. **Deselect all but one member of the interface redundancy group.**
4. **Select Lines > Change Lines.**

   The interface redundancy group no longer exists.
5. **Select File > Exit to exit the window.**

Note: You can find out whether interface redundancy is configured on a circuit by selecting that circuit in the Circuit Definition window and checking the Lines menu. If Interface Redundancy is grayed out, it is not configured on the circuit you selected.

Chapter 5
Configuring Router Redundancy

This chapter describes how to configure router redundancy. It assumes you have read *Configuring Routers* and Chapter 2 and Chapter 3 of this guide, and that you have already created a local configuration file for a router without router redundancy.

Note: You cannot configure router redundancy in dynamic or remote mode.

To enable router redundancy, you must select at least two routers as members of a router redundancy group. One of the routers will be the primary router; it will provide normal routing/bridging services. The other router will be the secondary, backup router; it will take over if the primary router fails.

When you enable router redundancy, you must configure some group and member global parameters. The Configuration Manager supplies default values for the remaining parameters. Use the directions that follow to enable router redundancy and edit router redundancy parameters.

For each parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

Enabling Router Redundancy

To configure a router redundancy group, you create a group configuration file. You then use this file as a template and apply it to each member of the group twice: once as a primary file, which the router uses when it boots as the primary member of the redundancy group, and then as a secondary file, which the router uses in its role as secondary member.

The instructions in this chapter assume that you want to create a router redundancy group consisting of two members: router *Alpha* and router *Beta*. The configuration file you apply to these routers is named *template*. This file can be an existing configuration file to which you are adding router redundancy, or it can be a new file you create to configure router redundancy and other features.

Creating a Group Configuration File

To create a redundancy group configuration file template, complete the following steps. All group members will use the values you configure in this file.

1. **In the main Site Manager window, select Tools > Router Redundancy > Group Configuration (Figure 5-1).**

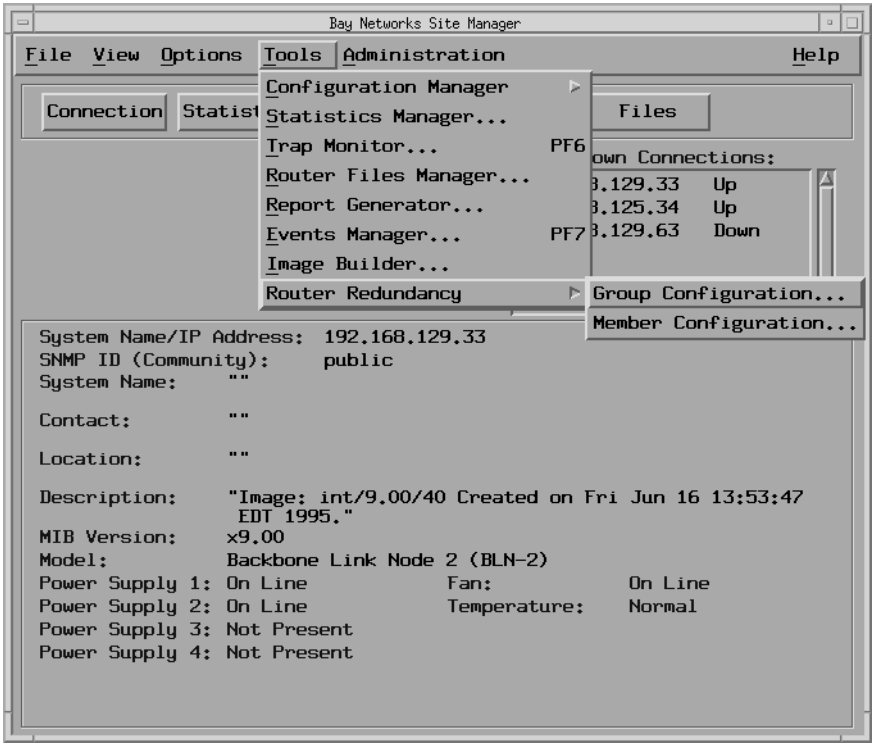

Figure 5-1. Main Site Manager Window

The standard file selection window appears.

2. **Enter *template* as the filename.**

   The standard router window appears.

3. **Select a router.**

   The Configuration Manager window appears.

4. **Select an empty slot.**

   The Module List window appears.

5. **Select a module and click on OK.**

   The Configuration Manager window appears.

6. **In the Configuration Manager window, select an available connector.**

The Add Circuit window appears (Figure 5-2).

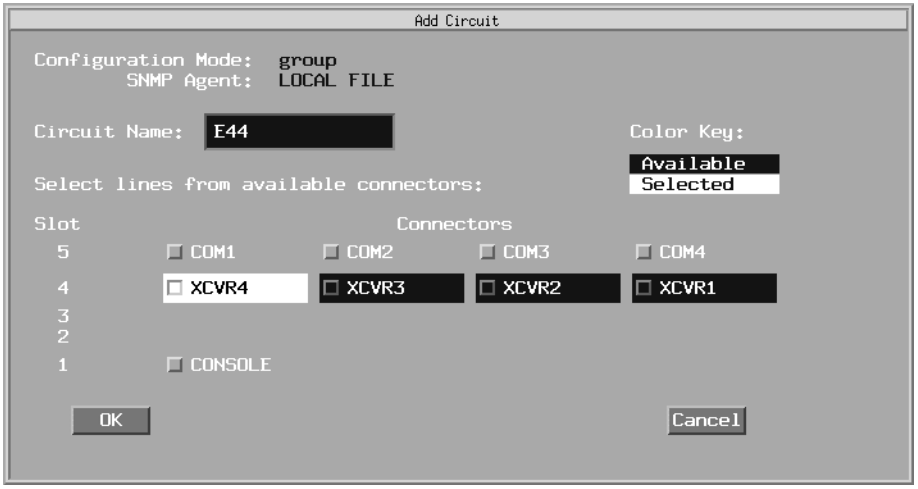

Figure 5-2. Add Circuit Window

7. **Select an available circuit that you want to configure for router redundancy. Click on OK.**

   The Select Protocols window appears (Figure 5-3).

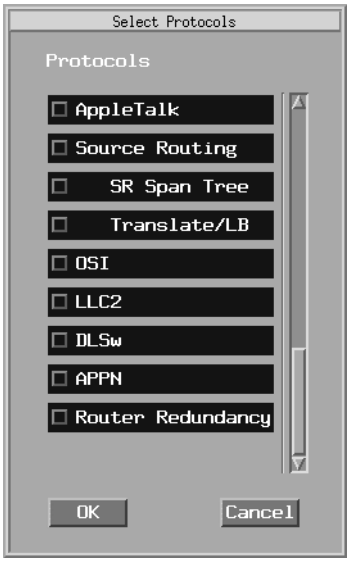

Figure 5-3. Select Protocols Window

8. **Scroll through the list and select Router Redundancy. You can also select other protocols that you want to configure.**
9. **Click on OK.**

   The Router Redundancy Circuit window appears (Figure 5-4).

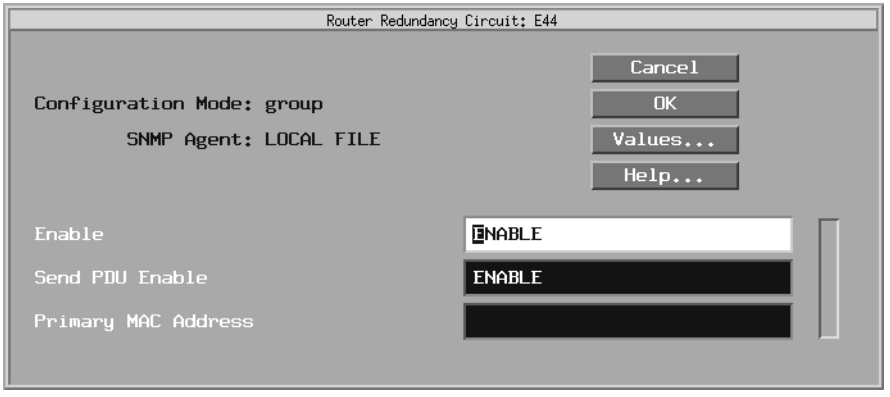

Figure 5-4. Router Redundancy Circuit Window

The Enable and Send PDU Enable parameters are set to Enable, as they must be for router redundancy to work.

Note: The Configuration Mode appears in the Configuration Manager window, the Add Circuit window, and the Router Redundancy Circuit window as “group.” You cannot add router redundancy to a circuit or edit redundancy parameters in any mode other than group mode.

10. **Enter the Primary MAC Address for the router (required).**

    Use the parameter description that follows these directions for guidelines.

11. **Click on OK.**

    The R.R. Group Global Parameters Configuration window appears (Figure 5-5).

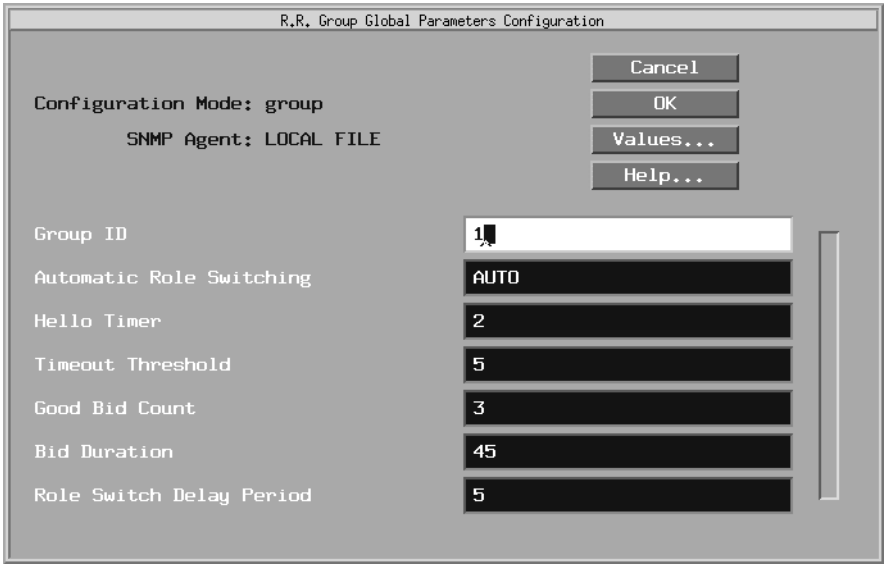

Figure 5-5. R.R. Group Global Parameters Configuration Window

Site Manager supplies default values for all parameters.

12. **Enter values for any parameters you want to edit, using the descriptions that follow this procedure for guidelines.**

13. **Click on OK.**

    The Configuration Manager window appears. The circuits you configured for router redundancy are either green or shaded, depending on your monitor.

14. **Select File > Save to exit the window.**

Router Redundancy Group Global Parameter Descriptions

Use the following descriptions as guidelines when you edit router redundancy group global parameters.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	This parameter is automatically set to Enable when you select Router Redundancy from the Select Protocols window. If you set this parameter to Disable, you temporarily disable the redundancy protocol on the router without deleting your configuration file.
Instructions:	Select Disable to stop the redundancy protocol from working on this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.2.1.2

Parameter:	**Send PDU Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables sending of router redundancy protocol data units (PDUs) on a per-circuit basis. This parameter is automatically set to Enable when you select Router Redundancy from the Select Protocols window. At least one interface on each router in the group must have this parameter enabled so that all routers in the group receive status information about each other. You may want to disable this parameter on some redundant interfaces to minimize network traffic on a busy interface.
Instructions:	Select Enable or Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.2.1.5

Parameter:	**Primary MAC Address**
Default:	None
Options:	Any unique, 48-bit MAC address that the network manager provides
Function:	The primary router uses the MAC address to route data. When the primary router fails and a backup router becomes the new primary router, the new primary router assumes this MAC address.
Instructions:	Enter a unique MAC address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.2.1.4

Note: If you are running DECnet on this interface, make sure the MAC address matches the MAC address used in the DECnet configuration.

Parameter:	**Group ID**
Default:	1
Range:	1 to 128
Function:	Specifies the identification number for the redundancy group. Each group ID number in a network must be unique.
Instructions:	Enter a number from 1 to 128 that you have not already assigned to a redundancy group on the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.4

Parameter:	**Automatic Role Switching**
Default:	Auto
Options:	Manual | Auto
Function:	Enables automatic role switching out of the primary role. When the primary router switches out of the primary role, a backup router switches into the primary role. Anything else that backup router has been doing stops when it becomes primary. In some circumstances, you may not want that stoppage to occur automatically. If that is the case, set this parameter to Manual. The warning section of the log will indicate when role switching is required.
Instructions:	Select Manual or accept the default of Auto.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.11

Parameter:	**Hello Timer**
Default:	2 seconds
Options:	1 through 86,400 seconds
Function:	Specifies the amount of time that the routers in the redundancy group have for sending each other primary and secondary Hello protocol data units (PDUs). The routers use Hello PDUs to initiate the bidding process that determines which router is primary.
Instructions:	Enter a value in the specified range or accept the default of 2.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.15

Parameter:	**Timeout Threshold**
Default:	5
Options:	1 through 100
Function:	Specifies the number of time periods during which the secondary routers wait to receive a Hello PDU from the primary router before they determine that the primary has failed.
Instructions:	Enter a number from 1 to 100 or accept the default of 5.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.17

Parameter:	**Good Bid Count**
Default:	3
Options:	1 through 10
Function:	Specifies the minimum number of good bids to become primary that are required from the same secondary router before Auto Role Switching occurs.
Instructions:	Enter a number from 1 to 10 or accept the default of 3.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.12

Parameter:	**Bid Duration**
Default:	45 seconds
Options:	1 through 65,535 seconds
Function:	Specifies the number of seconds during which routers bid to become primary router.
Instructions:	Select a value in the specified range or accept the default of 45. This value depends on how fast the router reboots with the configured features. For example, booting with FDDI interfaces, WAN interfaces with resources configured (such as servers and printers), OSPF, and so on, may require a larger value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.16

Parameter:	**Role Switch Delay Period**
Default:	5 seconds
Options:	1 through 86,400 seconds
Function:	Currently not used.
Instructions:	Accept the default.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.19

Configuring Resources

The redundancy protocol uses the Resource parameters to ensure that the primary router in the router redundancy group can reach the devices with which you have configured it to communicate. Use the procedure that follows to edit these parameters.

Although you can edit Resource parameters either in group mode or in member mode, usually it is best to configure Resource parameters in group mode because they are identical for all members of a router redundancy group. The exception is if you use router redundancy with wide area networks (refer to Example 3 in Appendix B). In this case you configure resources differently among members of a router redundancy group.

To edit Resource parameters:

1. **Select Protocols > Edit Router Redundancy > Resources in the Circuit Definition window.**

   The RREDUND Router Redundancy Resource List window appears (Figure 5-6).

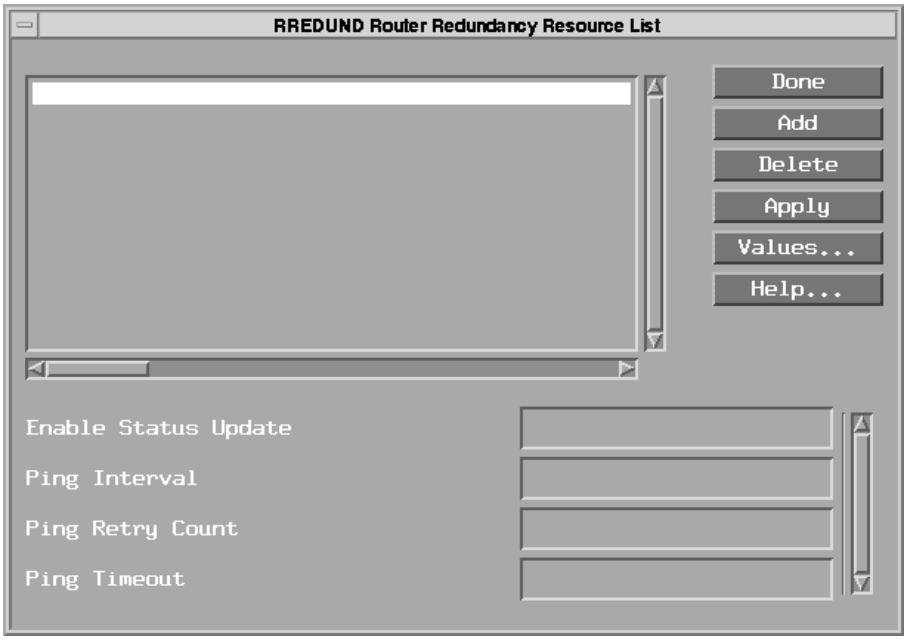

Figure 5-6. RREDUND Router Redundancy Resource List Window

2. **Click on Add.**

   The Router Redundancy Resource window appears (Figure 5-7).

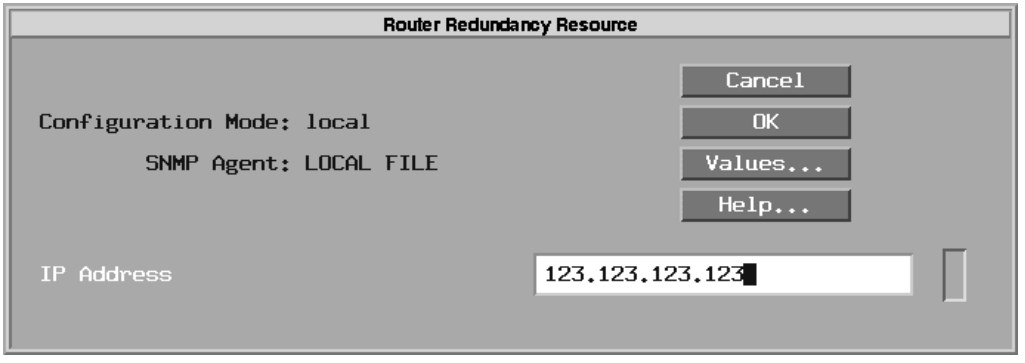

Figure 5-7. Router Redundancy Resource Window

3. **Enter the IP address of the device you want to configure as a resource for this router redundancy group.**
4. **Click on OK.**

   The RREDUND Router Redundancy Resource List window appears. The IP address you entered is highlighted in the list box. Site Manager supplies default values for all parameters.
5. **Enter values for any parameters you want to edit, using the descriptions that follow this procedure for guidelines.**
6. **Repeat Steps 2 through 5 to configure additional resources.**
7. **Click on Done to exit the window and return to the Circuit Definition window.**

Router Redundancy Resource Parameter Descriptions

Use the following descriptions as guidelines when you edit router redundancy resource parameters.

Parameter:	**Enable Status Update**
Default:	Enable
Options:	Enable | Disable
Function:	This parameter is automatically set to Enable when you select Router Redundancy from the Select Protocols window. If you set this parameter to Disable, you prevent the router from checking on the availability of the devices with which you configure it to communicate.
Instructions:	Accept the default, Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.3.1.6

Parameter:	**Ping Interval**
Default:	600 seconds
Options:	1 through 86,399 seconds
Function:	Specifies the amount of time, in seconds, that the router waits between attempts to ping the devices with which you configured it to communicate. The parameter applies when all is functioning normally.
Instructions:	Accept the default, or select another value in the specified range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.3.1.7

Parameter:	**Ping Retry Count**
Default:	3
Options:	1 through 9
Function:	Specifies the number of times that the primary router tries to ping a device before it determines that the device is unreachable.
Instructions:	Accept the default, or select another value in the specified range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.3.1.8

Parameter:	**Ping Timeout**
Default:	5 seconds
Options:	1 through 10 seconds
Function:	Specifies the amount of time, in seconds, that the router waits between attempts to ping the devices with which you configured it to communicate. This parameter applies when a prior ping has been unsuccessful.
Instructions:	Accept the default, or select another value in the specified range.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.3.1.9

Applying a Group Configuration File

To apply the group configuration file *template* to each member of a router redundancy group:

1. **In the main Site Manager window (refer to Figure 5-1), select Tools > Router Redundancy > Member Configuration.**

   The standard file selection window appears.

2. **Select the directory from which you created the file *template*, and select your configuration file, *template*.**

3. **Click on Open File.**

   The Configuration Manager window appears, but this time in member mode (Figure 5-8).

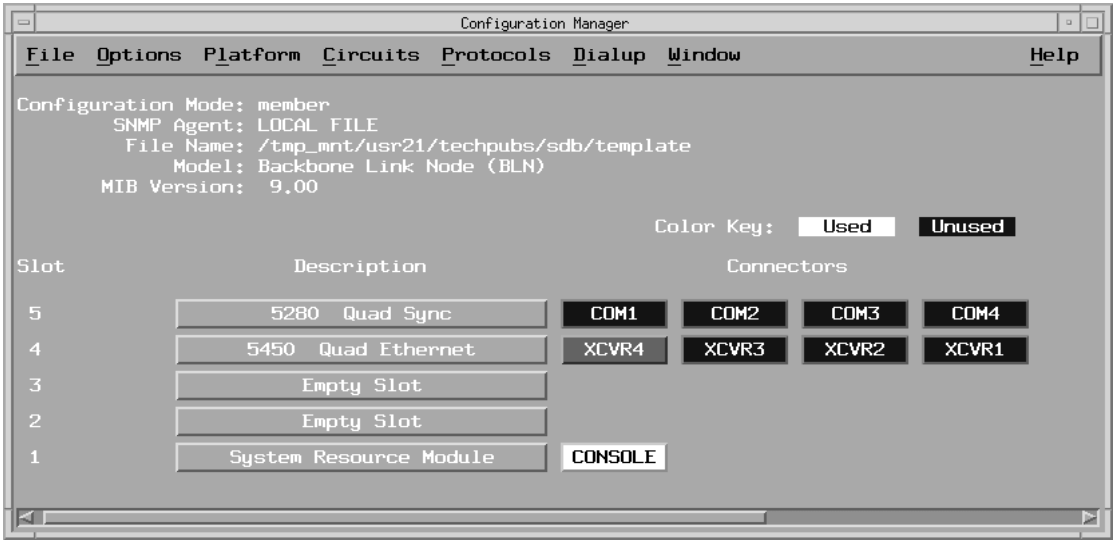

Figure 5-8. Configuration Manager Window in Member Mode

The circuit you previously selected for group configuration is shaded or in green.

4. **Select Protocols > Router Redundancy > Member Configuration in the Configuration Manager window (Figure 5-9).**

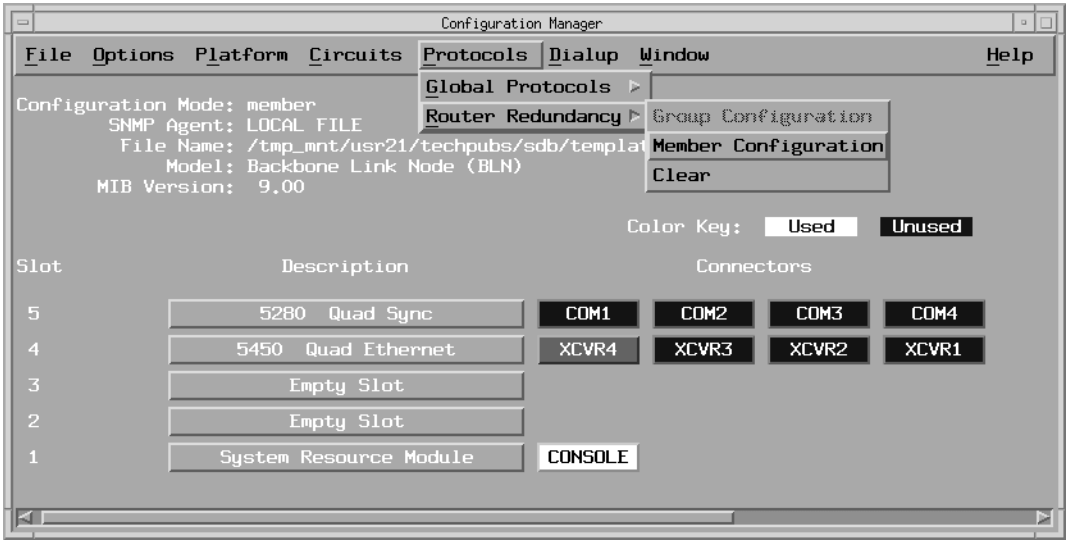

Figure 5-9. Configuration Manager Window for Member Configuration

Note: Select Protocols > Router Redundancy > Clear to clear all protocols except router redundancy from circuits with router redundancy configured. Use this feature when you are converting a primary configuration to a secondary one. See Steps 9 and 10 for further information.

The R.R. Member Global Parameters Configuration window appears (Figure 5-10).

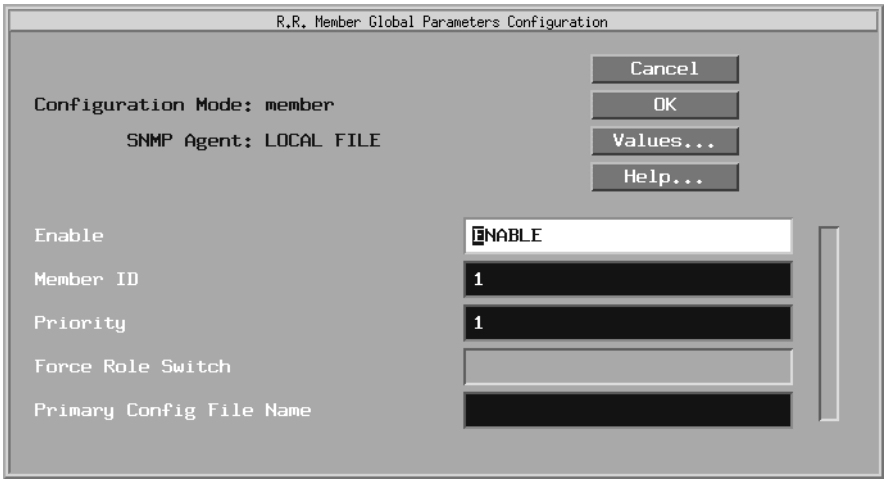

Figure 5-10. R.R. Member Global Parameters Configuration Window

5. **Enter values for the member global parameters, using the descriptions that follow this procedure for guidelines.**
6. **Click on OK when you are done.**

   The Configuration Manager window appears (refer to Figure 5-9).
7. **Select File > Save As.**

   The Save Configuration File window appears (Figure 5-11).

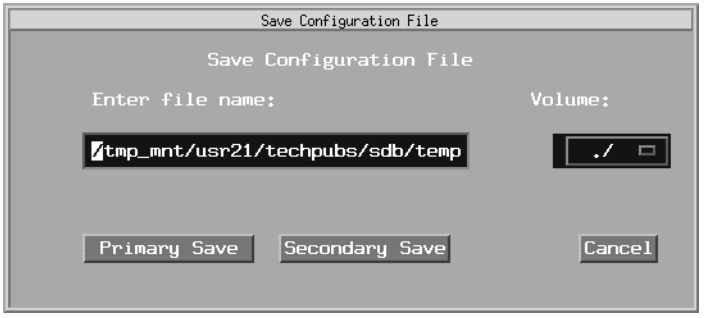

Figure 5-11. Save Configuration File Window

8. **Enter “Alpha” as the filename and click on Primary Save.**

   Site Manager appends the *.pri* suffix to the filename and then closes the window. The Configuration Manager window appears (refer to Figure 5-7).

9. **Select Protocols > Router Redundancy > Clear to clear all protocols except router redundancy from the redundant circuits.**

10. **Add any protocols you want to include in your secondary configuration file.**

11. **Select File > Save As in the Configuration Manager window.**

    The Save Configuration File window appears (refer to Figure 5-11).

12. **Again enter “Alpha” as the filename. Then click on Secondary Save.**

    Site Manager appends the *.sec* suffix to the filename and then closes the window.

13. **Exit from the Configuration Manager.**

If router Alpha and router Beta have identical configurations, you can now repeat Steps 1 through 13, using a different member ID and Beta as the base filename. If the configurations differ, you should modify the nonredundant parts of the configuration before saving the configuration file.

Router Redundancy Member Global Parameter Descriptions

Use the following descriptions as guidelines when you edit router redundancy member global parameters.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	This parameter is automatically set to Enable when you select Router Redundancy from the Select Protocols window. If you set this parameter to Disable, you temporarily disable router redundancy on the router without deleting your configuration file.
Instructions:	Select Disable to disable router redundancy on this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.2

Parameter:	**Member ID**
Default:	1
Options:	1 through 128
Function:	Specifies the identification number for this member of the router redundancy group. Each member ID number in a group must be unique. For example, if there are two routers in a redundancy group, one router could have a member ID of 1 and the other could have a member ID of 2. The role-change rules use the member ID to determine a router's priority to become the primary router if the Priority parameter for both routers is set to the same value.
Instructions:	Enter a number from 1 to 128 that you have not already assigned to a member of this redundancy group.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.5

Parameter:	**Priority**
Default:	1
Options:	1 through 128
Function:	Indicates this router's priority to become primary router; the higher the value, the higher the priority. The router with the highest priority becomes the primary router. If two routers have the same priority, the router with the lower member ID number has higher priority to become the primary router.
Instructions:	Enter a number from 1 to 128.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.14

Parameter:	**Force Role Switch**
Default:	Don't Switch
Options:	Don't Switch | Switch
Function:	Forces a router to switch out of the primary role when another member of the redundancy group would make a better primary router, or prevents a router from doing so. This parameter is valid only for manual role switching.
Instructions:	Select Don't Switch or Switch.
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.10

Parameter:	**Primary Config File Name**
Default:	None
Options:	A text string in DOS format, ***xxxxxxxx.xxx***
Function:	Specifies the name of the primary configuration file the router uses when it boots or reboots as the primary router. This filename is the one you enter with the Primary Save action described in Step 8 of the section "Applying a Group Configuration File," earlier in this chapter. The example in this guide uses the name *Alpha.pri*.
Instructions:	Enter a filename including the volume ID (required).
MIB Object ID:	1.3.6.1.4.1.18.3.5.17.1.20

Note: If a slot fails and the software cannot locate the primary configuration file and executable image on the volume you specified, the software searches all volumes to locate these files. We recommend that you store the image on multiple volumes to be readily available if a slot fails.

Sending the Configuration Files to the Routers

You have now created four configuration files for routers Alpha and Beta to use in their roles as primary and secondary members of a router redundancy groups. To send these files to the appropriate routers:

1. **Copy the files to a router's Flash card using FTP or TFTP.**

   Copy *Alpha.pri* and *Alpha.sec* to Alpha, and *Beta.pri* and *Beta.sec* to Beta.

2. **Copy** *Alpha.sec* **to the** *config* **file on the first router. Copy** *Beta.sec* **to the** *config* **file on the second router.**

Note: We recommend storing the template file on the routers as well.

Removing Router Redundancy

To remove router redundancy from a circuit or from an entire router:

1. **Create a new configuration file or modify the existing configuration file in local or remote mode.**
2. **Reboot the router.**

Appendix A
Site Manager Default Parameter Settings

This appendix lists the Site Manager default parameter settings for router redundancy group global parameters and member global parameters. Refer to Chapter 5 for instructions on editing these parameters.

Table A-1. Router Redundancy Group Global Parameters

Parameter	Default
Enable	Enable
Send PDU Enable	Enable
Primary MAC Address	None
Group ID	1
Automatic Role Switching	Auto
Hello Timer	2 s
Timeout Threshold	5
Good Bid Count	3
Bid Duration	45 s
Role Switch Delay Period	5 s

Table A-2. Router Redundancy Member Global Parameters

Parameter	Default
Enable	Enable
Member ID	1
Priority	1
Force Role Switch	Don’t Switch
Primary Config File Name	None

Table A-3. Router Redundancy Resource Parameters

Parameter	Default
Enable Status Update	Enable
Ping Interval	600 s
Ping Retry Count	3
Ping Timeout	5 s

Appendix B
Router Redundancy Examples

This appendix contains three examples of router configurations that use router redundancy.

Example 1: Two Routers at the Same Site

This example shows how router redundancy works in a configuration with two routers in the redundancy group, both in the same location. Figure B-1 illustrates two routers configured as a redundancy group in a Token Ring, Ethernet, or FDDI network.

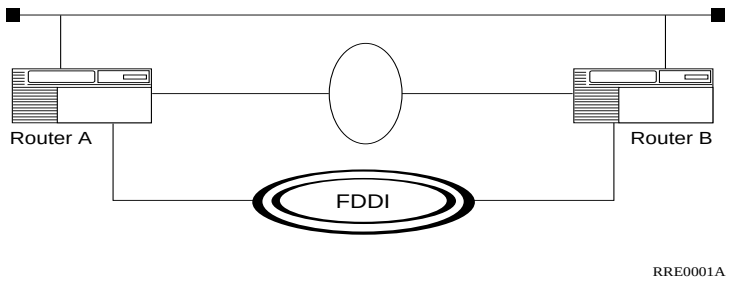

Figure B-1. Router Redundancy: Two Routers at the Same Site

Router Bootup

Upon router bootup, both members of the redundancy group are in the secondary role. They bid to determine which of the routers will assume the primary role (refer to Chapter 2). When the bidding time expires, the selected primary member switches into the primary role.

Possible Scenarios

The sections below describe possible scenarios and how they would affect the redundant routers.

Secondary Router Degraded

Degradation of the secondary router's interface and ability to reach resources does not affect the current operation of the primary router. This change does affect the primary and best-secondary selection process because the degraded secondary router has a lesser chance to become primary.

Secondary Router Becomes Inoperable

Degradation of the secondary router to the extent that it is inoperable does not affect the operation of the primary router. However, if the primary router detects local faults, it must remain primary and continue data transfer as best it can.

Primary Router Degraded

If the degree of degradation in the primary router is slight enough that the current primary router is still the best primary router, no change occurs.

If the degradation is such that the current primary router is no longer the best primary, role switch to a new primary may occur, depending on the availability of a secondary router, and on how you have set the Automatic Role Switching parameter. The primary and best-secondary selection process is the same as during initial bootup.

Primary Router Fails

The sudden failure of the primary router causes the best secondary router to switch roles to primary. Because the primary and best-secondary selection process is performed continuously and involves all members of the router redundancy group, no bidding process need occur at this time, and the switch occurs with minimal delay.

Possible Complications

Router Boots and Cannot Detect Another Member

If a member of a router redundancy group boots and cannot detect any other member of its redundancy group within the bidding period, it switches roles to become the primary router, because it is the only member from which to select the primary.

Second Router Boots After First Router's Bidding Timer Expires

If the first router has booted and a second router boots after the first router's bidding period expires, the first router may be in the process of switching roles to become the primary router. During the switching process, the first router does not send PDUs, so when the second router boots and begins its own bidding period, it may not detect the first router until the first router has completed the role switch. To avoid a situation in which both routers switch roles to become primary, set the bidding period for a longer time than the time required to perform a role switch.

Manual vs. Auto Role Switching

If the first router has booted and a second router boots after the first router's bidding period expires, and if you configured the router to use manual role switching, the first router continues to act as the primary router even if the second router would be a better primary. The software alerts you to the situation, and it is up to you to initiate the role switch. If you configure the router to use auto role switching, the routers perform the role switch automatically.

During manual role switching, a secondary router switches its role to primary if it does not detect a primary router in the group.

Example 2: Three Routers at the Same Site

Figure B-2 illustrates a router redundancy group with three routers at the same site.

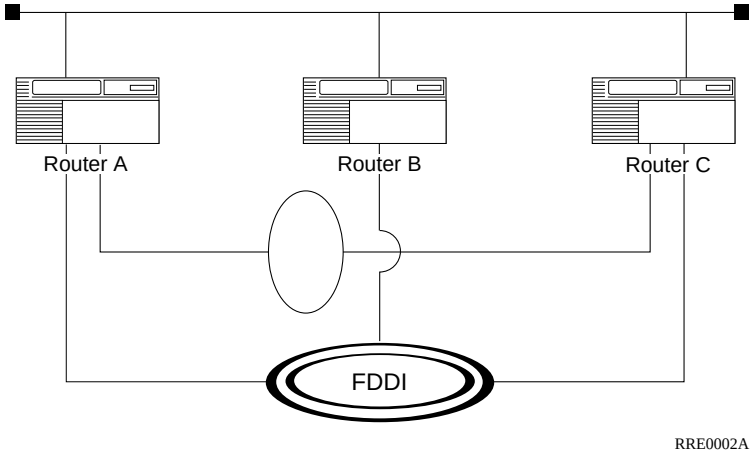

Figure B-2. Router Redundancy: Three Routers at the Same Site

The only difference between having two members and three members in a router redundancy group is that the best-secondary selection process becomes meaningful.

Any degradation of a secondary member may cause a new best secondary to be selected. Because the best-secondary selection process occurs upon any state change within the router redundancy group, the designation of the best secondary router is current at all times.

Example 3: Router Redundancy with Wide Area Networks

Bay Networks router redundancy services do not currently allow configuration of a wide area network (WAN) interface as a backed-up or redundant interface.

You can circumvent this limitation for IP-based networks only. Refer to Figure B-3 as you read the following explanation.

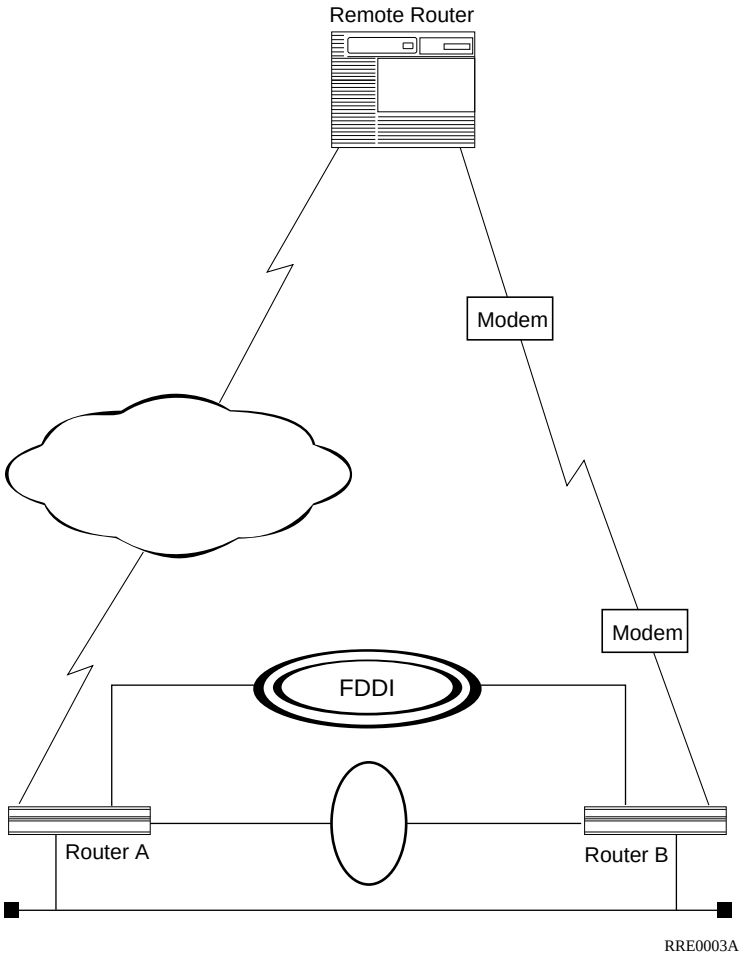

Figure B-3. Router Redundancy with Wide Area Networks

To provide redundancy for this wide area network (WAN):

1. **Define the remote interface on the other side of the WAN as a resource in the configuration of Router A.**

   This allows the primary and best-secondary router selection process to consider the WAN interface status, and to trigger role switching.

2. **Configure Router B to have a higher priority than Router A to become the primary router.**

If the WAN interface becomes nonfunctional for any reason, the resource defined for it is unreachable. This causes Router A, the current primary router, to cease being the best primary router, and a role switch occurs. Router B, with its dial-up connection, becomes the primary router.

The effect is that the dial-up connection is a redundant interface for the WAN connection. Note that in this case, you can disable the dial-up synchronous interface in the secondary configuration file on Router B and enable it in the primary configuration file to avoid the cost of two WAN connections to the remote router.

Router A and Router B can be at the branch office; the remote router is at the central or regional office.

Appendix C
Worksheets for Configuring Router Redundancy

These worksheets assume a router redundancy group of three routers. Use them to plan how to configure your router redundancy group.

Table C-1. Group Mode Planning Worksheet

Planning Issue/Parameter	Redundancy Group
Router Type All in group must be the same, for example, BCN, BLN, ASN	
Hardware Configuration CPU and interface module type, slot and port locations of the backed-up interfaces must be the same	
Software Configuration Software version and loadable modules configured must be the same	
Primary MAC Address for Backed-up Interfaces 1. 2. 3. 4.	
IP Addresses for Backed-Up Interfaces 1. 2. 3. 4.	
Group ID	
Automatic Role Switching	
Hello Timer	
Timeout Threshold	
Good Bid Count	
Bid Duration	

Table C-2. Resource Planning Worksheet

Planning Issue/Parameter	Router A	Router B	Router C
Enable Status Update			
Ping Interval			
Ping Retry Count			
Ping Timeout			
IP Addresses for Resources 1. 2. 3. 4.			

Table C-3. Member Mode Planning Worksheet

Parameter	Router A	Router B	Router C
Member ID			
Priority to Become Primary			
Force Role Switch			
Primary Configuration File Name			

Index

Symbols

100-Mb Ethernet, 3-2

10-Mb Ethernet, 3-2

A

active interface, defined, 1-1

adding interfaces to a group, 4-5

applying a group configuration file, 5-15

auto role switching, B-3

Automatic Role Switching parameter, 5-9, B-2

B

Bay Networks
- CompuServe forum, xx
- Customer Service FTP, xix
- home page on World Wide Web, xix
- InfoFACTS service, xxi
- publications, ordering, xv
- support programs, xviii
- Support Source CD, xx
- Technical Response Center, xvii, xxi
- technical support, xvii

Bid Duration parameter, 5-10

bidding period, B-3

bidding process for router redundancy, 2-2 to 2-5
- bypassing, 2-7

C

changing out of the primary role (router redundancy), 2-6

Clear function, 3-4, 5-16

compatibility, 3-4

CompuServe, Bay Networks forum on, xx

configuration examples for router redundancy, B-1 to B-6

configuration files
- applying to routers, 5-15
- creating, 5-2
- sending to the routers, 5-21

configuring
- interface redundancy, 4-1 to 4-6
- resources for redundant routers, 5-11 to 5-14
- router redundancy, 5-1 to 5-21
  - requirements, 3-2

Customer Service FTP, xix

customer support. *See* getting help

D

dedicated secondary router, defined, 2-1

deleting interfaces from a group, 4-5

designated primary interface, defined, 1-1

E

Enable parameter (group), 5-6, 5-7

Enable parameter (member), 5-18

Enable Status Update parameter (resource), 5-13

enabling
- interface redundancy, 4-1
- router redundancy, 5-2

examples of router redundancy configurations, B-1 to B-6

F

FDDI, 3-2
Force Role Switch parameter, 5-20

G

getting help
  from a Bay Networks Technical Response Center, xxi
  from the Support Source CD, xx
  through CompuServe, xx
  through Customer Service FTP, xix
  through InfoFACTS service, xxi
  through World Wide Web, xix
Good Bid Count parameter, 5-10
group configuration files
  applying, 5-15
  creating, 5-2
group configuration mode, 5-6
group global parameters
  Automatic Role Switching, 5-9
  Bid Duration, 5-10
  Enable, 5-7
  Good Bid Count, 5-10
  Group ID, 5-9
  Hello Timer, 5-9
  Primary MAC Address, 5-8
  Role Switch Delay Period, 5-11
  Send PDU Enable, 5-8
  Timeout Threshold, 5-10
Group ID parameter, 5-9

H

Hello Timer parameter, 5-9
hot standby, 1-3

I

implementation notes, 3-1
InfoFACTS service, xxi
interface failure in router redundancy, 2-6
interface redundancy
  adding or deleting interfaces, 4-5
  combined with router redundancy, 3-3
  configuring, 4-1 to 4-6
  hot standby, 1-3
  overview, 1-1
  priority rules, 1-2
  protocols supported, 3-2
  removing from a circuit, 4-6
  switching rules, 1-2
  warm standby, 1-3
IP, 3-2
IPX, 3-2

L

LAN interfaces
  100-Mb Ethernet, 3-2
  10-Mb Ethernet, 3-2
  FDDI, 3-2
  Token Ring, 3-2

M

manual role switching, B-3
member global parameters
  Enable, 5-18
  Force Role Switch, 5-20
  Member ID, 5-19
  Primary Config File Name, 5-20
  Priority, 5-19
Member ID parameter, 5-19
member mode, 5-15

N

network planning for redundancy services, 3-1, C-1

P

parameter default settings, A-1
PDU flow diagram, 2-2 to 2-5
PDUs, 2-2
Ping Interval parameter, 5-14
Ping Retry Count parameter, 5-14
Ping Timeout parameter, 5-14
planning your network for redundancy services, 3-1
Primary Config File Name parameter, 5-20
Primary MAC Address parameter, 5-8
primary router
  changing out of primary role, 2-6
  defined, 2-1
Priority parameter, 5-19
priority rules for interface redundancy, 1-2
protocol data units (PDUs)
  defined, 2-2
  used in role bidding, 2-2 to 2-5

R

redundancy protocol, 2-2 to 2-5
redundant interface, defined, 1-1
removing interface redundancy from a circuit, 4-6
removing router redundancy from a circuit or a router, 5-21
resource availability, 2-6
resource parameters
  Enable Status Update, 5-13
  Ping Interval, 5-14
  Ping Retry Count, 5-14
  Ping Timeout, 5-14
resources, configuring, 5-11 to 5-14
Role Switch Delay Period parameter, 5-11
router redundancy
  and wide area network (WAN) interfaces, B-5
  bidding process, 2-2 to 2-5
  combined with interface redundancy, 3-3
  configuration examples, B-1 to B-6
  configuring, 5-1 to 5-21
  dedicated secondary router, 2-1
  group global parameter descriptions, 5-7 to 5-11
  member global parameters descriptions, 5-18 to 5-20
  primary router, 2-1
  protocols supported, 3-2
  removing, 5-21
  requirements, 3-2
  resource parameter descriptions, 5-13 to 5-14
  role changes, 2-6
  worksheets, C-1

S

Send PDU Enable parameter, 5-6, 5-8
sending the configuration files to the routers, 5-21
software compatibility, 3-4
source route bridging, 3-2
spanning tree bridging, 3-2
Support Source CD, xx
switching rules for interface redundancy, 1-2

T

template, group configuration file, creating, 5-2
Timeout Threshold parameter, 5-10
Token Ring, 3-2

W

warm standby, 1-3
wide area network (WAN) interfaces and router redundancy, B-5
worksheets for router redundancy, C-1
World Wide Web, Bay Networks home page on, xix